



ISO 37301
golden standard for
compliance
management systems

Prof. Hernan Huwyler, MBA CPA





Agenda

Share ideas to use
the ISO 37301 in
internal audit

Advise on how to
implement changes
in the compliance
management
systems

Get new tools

- Compliance register
- Compliance risk model
- Anti retaliation controls

Answer to your
questions

The journey

ISO 26000:2010 | Guidance on social responsibility

ISO 37001:2016 Anti-bribery management systems

ISO 37002:2021 Whistleblowing management systems

ISO 19600:2014 Compliance management systems



ISO 37301:2021 Compliance management systems

ISO 37000:2021 Governance of organizations

Management Systems



Integration



Synergies

	ISO 37301	COSO Controls and Compliance
Scope	Auditable requirements	General principles
Integration	All management systems	Some internal audits
Process	Develop a compliance policy and audit controls of compliance management systems	Develop policies to address compliance and audit controls
Evaluation	Changes of compliance obligations	Changes in internal processes and strategy
Objective	Improve performance	Risk reduction

Corporate Defence

Evaluation of Corporate Compliance Programs by the US Department of Justice

	Strong	Weak
What methodology was used to assess compliance risks?	ISO 31022 with probabilistic models	Given by the consultants
What information was used to assess misconduct?	Data on non-compliances and control tests	Wet finger in the air
How compliance controls were balanced to risks?	To the quantified loss exposure	To the best efforts
How lessons learned are incorporated?	Retro test of losses against risks	I have a good memory
How do you understand the context?	Register of compliance obligations	Current activities

Register of Compliance Obligations



Ref	Area	Legislation title	Source	Scope	Owner	Relevance	Governance commentary
A001	Corruption	US Foreign Corrupt Practices Act	Law	Group	Group CPO	Prevent bribery activities involving US persons and non-US public officers	Supported by the ISO 37301 certification and whistleblowing line
B001	Systems	Data Processing Clauses	Contract	Client A	Contract Owner	Follow client's instructions in processing its personal data	
C001	Privacy	EU General Data Protection Regulation	Regulation	Group	Group DPO	Process customer and employees data only for business purposes with data security and legal controls	Supported by the ISO 27001 certification

Related aspects	Status	Policy	Effective date	Area of applicability	Impact	Controls	Records
Payment approvals, Due diligence	Maintain	Anti-bribery policy	Dec-77	Finance, Operations, Procurement	High	FA012 FA023 FA024 OS01 OS05	Pre-transaction anti-bribery due diligence, Corruption red flag analysis, High risk payment approvals
Service orders	Improve	Privacy policy	Jan-21	Data security, Operations	Low	IT04 IT05 OP43 PR01	Data processing agreement, Data deletion confirmation
Data security, Personal data inventory, Access management	Control	Privacy policy	May-18	Data security, DPO office	High	IT04 IT05 IT22 IT42 PR01 PR02 PR03 PR04 PR05	Privacy consents, Record of processing activities, Subject access requests, Data protection impact assessment



Register of Compliance Obligations



Training requirements	Authorizations, licenses and consents	Interested parties
Financial controllers and due diligence analysts to identify red flags for international corruption	None	US Department of Justice, Investors
Operation and IT staff to receive general data protection awareness	None	Client A, Sub-processors
Operation and IT staff to receive general data protection awareness	None	Norwegian Datatilsynet

Compliance risk



ISO 31000 and 31022

Best available information

**Balance costs of actions to
expected loss exposure**

Consider biases

Disregarding Scientific Evidence is Malpractice

What is wrong about risk matrices, Tony Cox, 2008 > **worse than useless**

Further thoughts on the utility of risk matrices, David Ball, 2013 >

untrustworthy picture

Some extensions on risk matrix approach, Huihui Ni, 2010 > **defects still left unresolved**

On the origin of probability consequence diagrams, Ben Ale, 2015 > **single factor impacts**

Problems with scoring methods and ordinal scales, Doug Hubbard, 2010 > **arbitrary features of the scoring**

Recommendations on the use and design of risk matrices, Niels Duijm, 2015 > **aggregation is problematical**

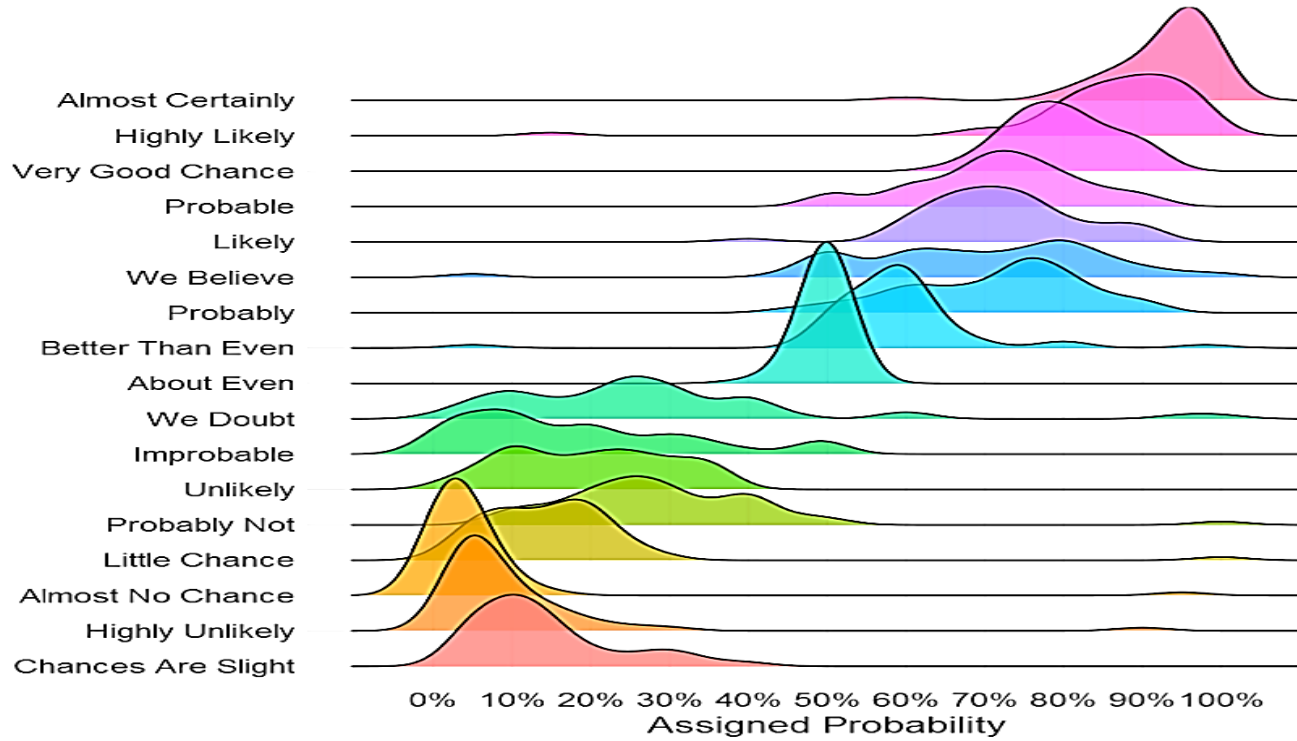
Back to Basics: Risk Matrices and ALARP, Glen Wilkinson, 2010 > **unable to compare risks**

Qualitative Criteria

Scale	Existing controls	Frequency of noncompliance
5 Almost certain	<ul style="list-style-type: none"> • No controls in place • No policies or procedures, no responsible person(s) identified, no training, no management review 	<p>Expected to occur in most circumstances</p> <p>More than once per year</p>
4 Likely	<ul style="list-style-type: none"> • Policies and procedures in place but neither mandated nor updated regularly • Controls not tested or tested with unsatisfactory results • Responsible person(s) identified • Some formal and informal (on-the-job) training • No management reviews 	<p>Will probably occur</p> <p>At least once per year</p>
3 Possible	<ul style="list-style-type: none"> • Policies mandated, but not updated regularly • Controls tested only occasionally, with mixed results • Responsible person(s) identified • Training is provided when needed • Occasional management reviews are performed, but not documented 	<p>Might occur at some time</p> <p>At least once in 5 years</p>
2 Unlikely	<ul style="list-style-type: none"> • Policies mandated and updated regularly • Controls tested with mostly positive results • Regular training provided to the identified responsible person(s), but not documented • Regular management reviews are performed, but not documented 	<p>Could occur at some time</p> <p>At least once in 10 years</p>
1 Rare	<ul style="list-style-type: none"> • Policies mandated and updated regularly • Controls regularly tested with positive results • Regular mandatory training is provided to the identified responsible person(s), and the training is documented • Regular management reviews are performed and documented 	<p>May occur only in exceptional circumstances</p> <p>Less than once in 10 years</p>

* Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 30.


Words of Estimative Probability



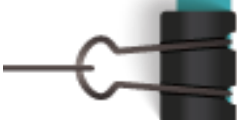
Risk is Decision-Making




Is this bidding price covering the liabilities of this contract?




What is the threshold to escalate this approval?




How much should the legal reserve be for this new service?



Should this potential supplier be selected at this price?

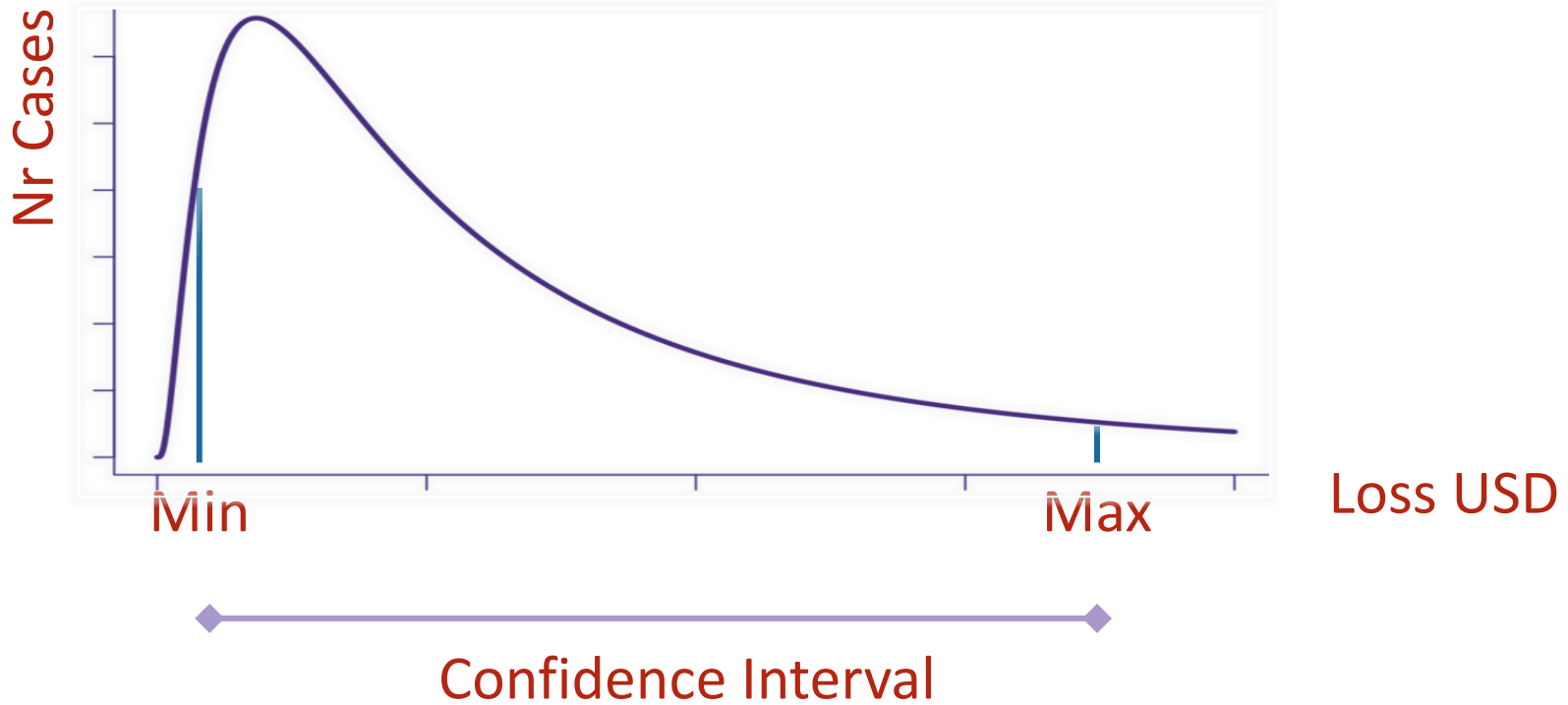


Is this insurance coverage en




What is the best strategy to deal with this customer claim?

Methodology



Methodology

$$\text{Single Loss USD} = \text{Ln} \left(P(A), \mu = \frac{\text{Ln (Max)} + \text{Ln (Min)}}{2}, \sigma = \frac{\text{Ln (Max)} - \text{Ln (Min)}}{\text{Standard Error}} \right)$$

 =LOGNORM.INV(RAND(),(LN(Max)+LN(Min))/2,(LN(Max)-LN(Min))/standard error))

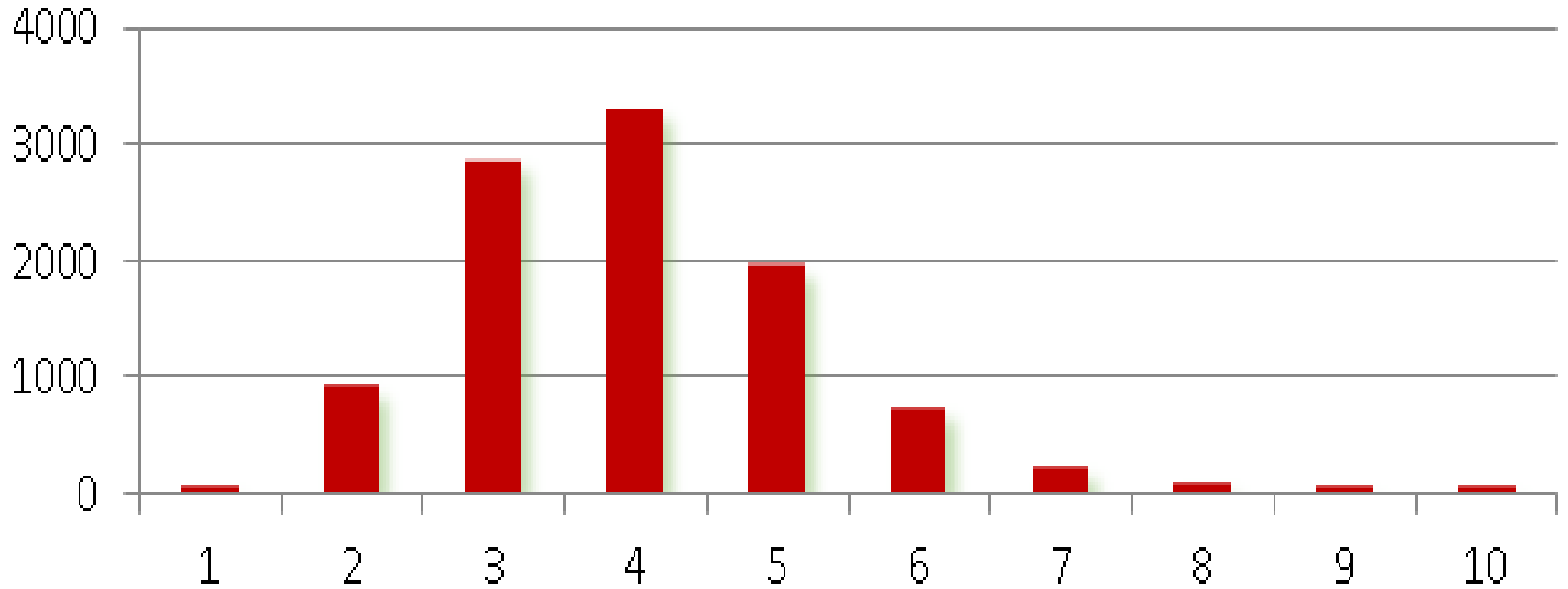
z*-value*2	Confidence Interval	Standard Error
	80%	2.56
	90%	3.29
	95%	3.92
	99%	5.15

Methodology



Requirement	Analysis	Values
1 -	Max Loss per Event	0
	Min Loss per Event	0
	Confidence	99%
	Highest Possible Loss	99,999,999
	Lowest Possible Loss	0
	Max Probability per Year	0.0%
	Min Probability per Year	0.0%
	Confidence	99%

Methodology



Methodology



Bin	ALE	Acum	Frequency
0	0	0	0
1	0	32	32
2	0	928	896
3	0	3781	2853
4	0	7076	3295
5	0	9016	1940
6	0	9729	713
7	0	9928	199
8	0	9985	57
9	0	9997	12
10	0	9998	2
11	1	10000	0

Reserve 50% 0

Max 0

Min 0

Median 0

Average 0

Reserve 50% 0



01

Add compliance obligations in procedures and job descriptions

02

Cover compliance controls in performance appraisals and incentives

03

Analyze root-causes of compliance violations

04

Validate quality and availability of compliance documentation

05

Assess the effectiveness of compliance training and awareness



Anti-retaliation controls



- **Implement a leniency program**
- **Have an independent investigative team**
- **Prevent risks in the complaint ramifications**
- **Monitor peer pressure, bullying and exclusion**
- **Approve changes in work conditions**
- **Include the impact on family members**
- **Provide financial and emotional support**
- **Protect whistleblowers from 3 to 5 years**

<https://donate.unhcr.org/int/en/ukraine-emergency>



Secure Donation

English



How would you like to donate?

One-off

Monthly

US\$ 500

US\$ 150

US\$ 50





Let's connect



[/in/hernanwyler](#)



[hewyler](#)